IB/2004/02168

Sertifikaat

REPUBLIEK VAN SUID AFRIKA

PATENT KANTOOR
DEPARTEMENT VAN HANDEL
EN NYWERHEID

Certificate

REPUBLIC OF SOUTH AFRICA

PATENT OFFICE
DEPARTMENT OF TRADE AND
INDUSTRY

Hiermee word gesertifiseer dat
This is to certify that

the documents attached hereto are true copies of Forms P1, P2 and provisional specification and drawing of South African Patent Application No. 2003/5050 in the name of Holdsworth John Charles and an applicant substituted to JHA I – Commerce (Pty) Ltd on 29 June 2004

Filed : 30 June 2003 ✓

Entitled : Systems and Methods for the Authentication of Transactions Initiated from Non-Internet Enabled Devices

Geteken te PRETORIA in die Republiek van Suid-Afrika, hierdie 13th dag van July 2004
Signed at PRETORIA in the Republic of South Africa, this 13th day of July 2004

Registrar of Patents

FORM P 2

(To be lodged in duplicate)

REPUBLIC OF SOUTH AFRICA

PATENTS ACT, 1978

REGISTER OF PATENTS

Official application No.	Lodging date: Provisional	Acceptance date
21 2003/5050	22 2003 -06- 30	47
International classification	Lodging date: Complete	Granted date
51	23	

Full name(s) of applicant(s)/Patentee(s):

71 HOLDSWORTH : JOHN CHARLES

Applicants substituted:	Date registered
71 JHA I-COMMERCE (PTY) LTD	29-6-04.
Assignee(s):	Date registered
71	

Full name(s) of inventor(s):

72 HOLDSWORTH : JOHN CHARLES

Priority claimed	Country	Number	Date
	3	3	3
	3	3	3
	3	3	3

Title of invention

54 SYSTEMS AND METHODS FOR THE AUTHENTICATION OF TRANSACTIONS INITIATED FROM NON-INTERNET ENABLED DEVICES

Address of applicant(s)/Patentee(s) 24, EDEN GARDENS, KOLLEGE ROAD, ALLEN GROVE, KEMPTON PARK, GAUTENG, SOUTH AFRICA

Address for service Spoor + Fisher ~~24, EDEN GARDENS, KOLLEGE~~ ROAD, ALLEN GROVE, KEMPTON PARK, 1619,

74 GAUTENG, SOUTH AFRICA.

Patent of addition No.	Date of any change	
61		
Fresh application based on	Date of any change	

P 015 (E)

G.P.-S. 019-0126

REPUBLIC OF SOUTH AFRICA

PATENTS ACT, 1978

PO 32 E
Form P I

APPLICATION FOR A PATENT AND ACKNOWL

[Section 30 (I)-Regula

(See notes overleaf

The grant of a patent is hereby requested by the undermentioned applicant on the basis of the present application filed in duplicate.

Official Application No.	
	2003/5050

(i) Applicant's or agent's reference

(ii) AANSOEKERS VERVANG 29/6/04
APPLICANTS SUBSTITUTED

71 Full name(s) of applicant(s) HOLDSWORTH : JOHN CHARLES

(iii) JHA I-COMMERCE (PTY) LTD

Address(es) of applicant(s) 24, EDEN GARDENS, KOLLEGE ROAD, ALLEN GROVE, KEMPTON PARK, 1619, GAUTENG, SOUTH AFRICA.

(iv)
54 Title of invention SYSTEMS AND METHODS FOR THE AUTHENTICATION OF TRANSACTIONS INITIATED FROM NON-INTERNET ENABLED DEVICES

(v)
□ The applicant claims priority as set out on the accompanying form P 2.

(vi)
□ This application is for a patent of addition to Patient Application No.

(vii)
□ This application is a fresh application in terms of section 37 and based on Application No.
21

(viii)
This application is accompanied by:

✓	1.	A single copy of a provisional ~~or two copies of a complete~~ specification of 16 pages.
✓	2.	Drawings of 2 sheets.
	3.	Publication particulars and abstract (form P 8 in duplicate).
	4.	A copy of Figure .... of drawings (if any) for the abstract.
	5.	An assignment of invention.
	6.	Certified priority document(s) (state number).
	7.	Translation of the priority document(s).
	8.	An assignment of priority rights..
	9.	A copy of the form P 2 and the specification of S.A. Patent Application
✓	10.	A declaration and Power of Attorney on form P 3.
	11.	Request for ante-dating on form P 4.
	12.	Request for classification on form P 9.
	13.	

(ix)
74 Address for service: Spoor + Fisher
~~24, EDEN GARDENS, KOLLEGE ROAD, ALLEN GROVE, KEMPTON PARK, 1619, GAUTENG, SOUTH AFRICA~~

Dated this 30TH day of JUNE 2003

Signature of applicant(s) or agent

The duplicate will be returned to the applicant's address for service as proof of lodging but is not valid unless endorsed with official stamp.

FORM P.3

REPUBLIC OF SOUTH AFRICA
PATENTS ACT, 1978
DECLARATION AND POWER OF ATTORNEY
(Section 30 - Regulation 8, 22(i)(c) and 33)

PATENT APPLICATION NO

21	01	2003/5050

REF:

LODGING DATE

22	2003 -06- 30

FULL NAME(S) OF APPLICANT(S)

71	HOLOSWORTH : JOHN CHARLES

FULL NAME(S) OF INVENTOR(S)

72	HOLOSWORTH : JOHN CHARLES

EARLIEST PRIORITY CLAIMED	COUNTRY		NUMBER		DATE	
	33		31		32	

NOTE: The country must be indicated by its International Abbreviation - see schedule 4 of the Regulations

TITLE OF INVENTION

54	SYSTEMS AND METHODS FOR THE AUTHENTICATION OF TRANSACTIONS INITIATED FROM NON-INTERNET ENABLED DEVICES

* I/~~We~~ JOHN CHARLES HOLOSWORTH

hereby declare that :-

* 1 I/~~we~~ am/~~are~~ the applicant(s) mentioned above;

** ~~2.~~ I/we have been authorized by the applicant(s) to make this declaration and have knowledge of the facts herein stated in the capacity of of the applicant(s);

*** 3 the inventor(s) of the abovementioned invention is/~~are~~ the person(s) named above ~~and the applicant(s) has/have acquired the right to apply by virtue of an assignment from the inventor(s);~~

4 to the best of my/our knowledge and belief, if a patent is granted on the application, there will be no lawful ground for the revocation of the patent;

*** ~~5.~~ this is a convention application and the earliest application from which priority is claimed as set out above is the first application in a convention country in respect of the invention claimed in any of the claims; and

~~6.~~ the partners and qualified staff of the firm of , patent attorneys, are authorised, jointly and severally, with powers of substitution and revocation, to represent the applicant(s) in this application and to be the address for service of the applicant(s) while the application is pending and after a patent has been granted on the application.

SIGNED AT KEMPTON PARK THIS 30TH DAY OF JUNE 2003

SIGNATURE(S)
(no legalization necessary)

** In the case of application in the name of a company, partnership or firm, give full names of signatory/signatories, delete paragraph 1, and enter capacity of each signatory in paragraph 2.

*** If the applicant is a natural person, delete paragraph 2.

**** If the right to apply is not by virtue of an assignment from the inventor(s), delete "an assignmnt from the Inventw(s)" and give details of acquisition of right.

For non-convenuon applications, delete paragraph 5.

Form P6

REPUBLIC OF SOUTH AFRICA

PATENTS ACT, 1978

PROVISIONAL SPECIFICATION

(Section 30(I) - Regulation 27)

Official Application No.

21 01 2003/5050

Lodging Date

22 2003 -06- 30

Full name(s) of applicant(s)

71 HOLDSWORTH : JOHN CHARLES

09-6-04

AANSOEKERS VERVANG
APPLICANTS SUBSTITUTED

JHA I-COMMERCE (PTY) LTD

Full name(s) of inventors(s)

72 HOLDSWORTH : JOHN CHARLES

Title of invention

54 SYSTEMS AND METHODS FOR THE AUTHENTICATION OF TRANSACTIONS INITIATED FROM NON-INTERNET ENABLED DEVICES

Patent

SPECIFICATION

SYSTEMS AND METHODS FOR THE AUTHENTICATION OF TRANSACTIONS INITIATED FROM NON-INTERNET ENABLED DEVICES

1. Field of the Inventions

[001] The field of the invention relates generally to mobile payments and more specifically to the authentication of mobile payment transactions initiated from non-internet enabled devices.

2. Background Information

[002] Mobile telecommunications continues to be very successful, with an estimated one billion mobile subscribers by the end of 2002 (Source: The Universal Mobile Telecommunications Service (UMTS) Forum. The success of NTT DoCoMo's i-mode service in Japan, which currently has 34 million data subscribers, illustrates the appetite for compelling mobile data services. In CEMEA the viral uptake of short messaging services (SMS) has demonstrated the huge demand for non-voice services in those markets. A joint survey by Visa International and Boston Consulting predicts that combined e-commerce and m-commerce volumes will grow from $38 billion in 2002 to $128 billion in 2004.

[003] In the meantime, high speed data networks, with more sophisticated wireless devices have the ability to transform mobile payment. Greater bandwidth, larger screens, colour displays, longer battery life and compelling content are converging to create an environment where consumers can purchase services and products on the move. However, the success of both e-commerce and m-commerce is contingent on the same factors that have fuelled the growth of physical payments namely security and privacy. Virtual payments, whether executed via a personal computer or a mobile phone must be subject to the same

common standards that govern physical payment card use in order to be perceived as familiar and secure.

[004] In response to this need, the card associations have developed new online cardholder authentication standards and have globally mandated that from the 1st of April 2003, Acquirers of payment card transactions must offer to their online merchants the new standards such as the 3-Domain Secure (3-D Secure™) protocol which has been developed by Visa International and licensed to MasterCard. The objectives are to provide Issuers with the ability to authenticate cardholders during an online purchase. This will enable all parties in an on-line transaction to transmit confidential and correct payment data and provide authentication that the buyer is an authorized user of a particular card.

SUMMARY OF THE INVENTION

[005] The 3-D Secure™ protocol specification defines an architecture and protocol for authenticating cardholders during Internet-based transactions. After initiating the final purchase action, the cardholder is placed into a dialogue with his issuing financial institution. The issuer authenticates the cardholder and sends a proof of identity back to the merchant; the merchant completes the transaction.

[006] The 3-D Secure™ protocol was designed for the support of "Internet shopping", where the cardholder is shopping using their Internet-enabled device, and the authentication takes place over the Internet. However, the purchase and authentication can be performed using non-internet enabled devices and certain interactive technologies such as Interactive Voice Response (IVR), Short Message Services (SMS), SIM Toolkit (STK), Unstructured Supplementary Services Data (USSD) and Wireless Application Protocol (WAP) that have more limited capabilities.

[007] This invention defines systems and methods that enable Issuers, Acquirers and Merchants to use the 3-D Secure™ online cardholder authentication protocol to authenticate cardholders transacting with non-internet enabled devices. The invention operates as a proxy on behalf of the cardholder and simulates a core 3-D Secure™ session to the Merchant Plug-in (MPI) and Issuer Access Control Server (ACS). That is, it converts voice or data based messages received from non-internet enabled devices into a format that is consistent with the requirements of the 3-D Secure™ protocol. Further, the invention can be implemented without Issuers, Acquirers or Merchants having to upgrade or enhance infrastructure.

BRIEF DESCRIPTION OF THE DRAWINGS

[008] Features, aspects, and embodiments of the inventions are described in conjunction with the attached drawings, in which:

[009] Figure 1 is a diagram illustrating an online cardholder authentication system in accordance with an example embodiment of the invention;

[010] Figure 2 is a diagram illustrating the online cardholder authentication system of figure 1 in more detail, configured in accordance with an example embodiment of the invention;

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[011] To help better understand the systems and methods described herein, a specific example involving a transaction initiated from a non-internet enabled device over a wireless and wired network is examined below.

[012] **Figure 1** is a diagram illustrating an example embodiment of an online cardholder authentication system 100 configured in accordance with one embodiment of the systems and methods described herein. System 100 comprises a non-internet enabled device 101 that is configured to communicate through a wired and/or wireless network 102 with a mobile Operator Server 103. System 100 also comprises a Virtual Cardholder System 104, a Merchant Plug-in 105, a Card Association Directory Service 106; and an Issuer Access Control Server 107;

[013] Device 101 can be any type of device configured to communicate over a wired and/or wireless network, including but not limited to a land-line, mobile phone, personal digital assistant or laptop computer.

[014] Network 102 can be any type of Internet, GSM, CDMA, TDMA, GPRS, 3G, Bluetooth, Infrared, RFID wired and/or wireless network, configured to support a range of interactive technologies including but not limited to Voice, SMS, STK, USSD, WAP and i-mode.

[015] Accordingly, mobile Operator Server 103, Card Association Directory Service 106 and Issuer Access Control Server 107 can be any type of server configured to support the above, non-internet enabled devices, wireless network protocols and interactive technologies;

[016] **Figure 2** is a flow chart illustrating an example online cardholder authentication process according to one embodiment of the system and methods described

herein. The process begins in step 201 when a cardholder dials a telephone number and submits a purchase request over network 102 to Operator Server 103 using an appropriate interactive technology.

[017] In step 202 Operator Server 103 formats a message and sends it to Virtual Cardholder System 104 via a secure channel i.e. SSL, IPSec. The secure channel between Operator Server 103 and Virtual Cardholder System 104 is typically but not always a dedicated leased line.

[018] In step 203 Virtual Cardholder System 104 extracts a unique identifier associated with non-internet enabled device 101 from the message, matches it with a corresponding value stored on a database, extracts the primary account number (PAN), Expiry Date and Card Verification Value (CVV) if credit, retrieves the Merchant Plug-in URL from the message and simulating an Internet browser starts an http/s session with Merchant Plug-in 105.

[019] In step 204 Merchant Plug-in 105 formats a message and queries Card Association Directory Service 106 on the enrollment status of the PAN.

[020] In step 205 if the PAN is in participating card range, Card Association Directory Service 106 queries the Issuer Access Control Server 107 to determine whether the PAN is enrolled. Issuer Access Control Server 107 formats a message and responds to the Card Association Directory Service 106 with PAN participation information.

[021] In step 206 Card Association Directory Service 106 forwards the Issuer Access Control Server response to Merchant Plug-in 105.

[022] In step 207 Merchant Plug-in 105 sends a message to Issuer Access Control Server 107 via Virtual Cardholder System 104.

[023] In step 208 Virtual Cardholder System 104 acting on behalf of the cardholder simulates an Internet browser and posts the message to Issuer Access Control Server 107. Issuer Access Control Server 107 responds by sending an HTML purchase authentication page to Virtual Cardholder System 104.

[024] In step 209 Virtual Cardholder System 104 extracts displayable information, stores the HTML page and formats a message which it sends to Operator Server 103.

[025] In step 210 Operator Server 103 translates the message to a format that device 101 understands and requests that the cardholder enter his credentials.

[026] In step 211 the cardholder enters his credentials using the appropriate interactive technology and sends it to Operator Server 103.

[027] In step 212 operator system 103 converts the message to a format that Virtual Cardholder System 104 understands and sends a message containing the cardholder credentials to Virtual Cardholder System 104.

[028] In step 213 Virtual Cardholder System 104 acting on behalf of the cardholder extracts the cardholder credentials from the message; parses the stored HTML page recognizing the cardholder credentials field; inserts the cardholder credentials in the appropriate field and posts the HTML purchase authentication page to the Issuer server 107. Issuer Access Control Server 107 accepts the cardholder credentials; authenticates it against the account holder database and responds to virtual access control server 107 with an authentication response message.

[029] In step 214 Virtual Cardholder System 104 simulating an Internet browser forwards the authentication response message to Merchant Plug-in 105.

[030] In step 215 Merchant Plug-in 105 receives and decodes the authentication response, validates the digital signature, generates an authorization request message and sends it to an acquirer. Merchant Plug-in 105 receives the authorization response message from the acquirer and forwards it to Virtual Cardholder System 104.

What is claimed:-

1. A method for authenticating a transaction initiated from a non-internet enabled device; comprising:

- A Cardholder submitting a purchase request message from a non-internet enabled device over a network using an appropriate interactive technology;
- An Operator Server converting the purchase request message from the protocol used by the interactive technology to a standard Internet format;
- A Virtual Cardholder System extracting a unique identifier from the purchase request message and matching it with a corresponding value stored in a remote database;
- A Virtual Cardholder System extracting cardholder data (PAN, expiry date, CVV) stored in the remote database;
- A Virtual Cardholder System retrieving the Merchant Plug-in URL from the purchase request message;
- A Virtual Cardholder System simulating an Internet browser and starting an http/s session with the Merchant Plug-in;
- A Merchant Plug-in formatting a message and querying a Card Association Directory Service on the enrollment status of the PAN;
- A Card Association Directory Service querying an Issuer Access Control Server to determine if PAN is enrolled;
- An Issuer Access Control Server formatting a message and responding to the Card Association Directory Service with PAN participation information;

- A Card Association Directory Service forwarding the Issuer Access Control Server response to the Merchant Plug-in;
- A Merchant Plug-in sending a message to the Issuer Access Control Server via the Virtual Cardholder System;
- A Virtual Cardholder System simulating an Internet browser and posting an authentication request message to the Issuer Access Control Server;
- An Issuer Access Control Server responding by sending an HTML purchase authentication page to the Virtual Cardholder System;
- A Virtual Cardholder System receiving the HTML authentication request page from the Issuer Access Control Server;
- A Virtual Cardholder System extracting displayable information and storing the HTML authentication request page;
- An Operator Server requesting the cardholder enter his credentials using an appropriate interactive technology;
- An Operator Server converting the cardholder credentials from the protocol used by the appropriate interactive technology to a standard Internet format;
- A Virtual Cardholder System parsing the stored HTML authentication request page and recognizing the cardholder credential field(s);
- A Virtual Cardholder System acting on behalf of the cardholder and inserting the credentials into the HTML authentication request page;
- A Virtual Cardholder System simulating an Internet browser and posting the HTML authentication request page to an Issuer Access Control Server;

- An Issuer Access Control Server authenticating the cardholder credentials against an account holder database;
- An Issuer Access Control Server responding to the Virtual Cardholder System with an authentication response message;
- A Virtual Cardholder System receiving the authentication response message from the Issuer Access Control Server;
- A Virtual cardholder System simulating an Internet browser and forwarding the authentication response message to the Merchant Plug-in;
- A Merchant Plug-in decoding the authentication response and validating the digital signature;
- A Merchant Plug-in generating an authorization request message and sending it to a Gateway, Processor or Acquirer;
- A Gateway, Processor or Acquirer proceeding with the conventional purchase authorization process;
- A Merchant Plug-in receives an authorization response message from the acquirer and forwards it to the Virtual Cardholder System
- A Virtual Cardholder System forwarding the authorization response message to the Operator Server;
- An Operator Server converting authorization response message from a standard Internet format to protocol used by the appropriate interactive technology;

2. The method of claim 1, further comprising using a plurality of non-internet enabled devices to capture a purchase request, wherein a mobile phone is just one of the plurality of non-internet enabled devices.

3. The method of claim 2, wherein the plurality of non-internet enabled devices includes a landline telephone.

4. The method of claim 2, wherein the plurality of non-internet enabled devices includes a Personal Digital Assistant (PDA).

5. The method of claim 2, wherein the plurality of non-internet enabled devices includes a laptop computer.

6. The method of claim 1, further comprising, using a plurality of interactive technologies to submit a purchase request, wherein an Interactive Voice Response (IVR) is just one of the plurality of interactive technologies.

7. The method of claim 6, wherein the plurality of interactive technologies includes Interactive Voice Response (IVR).

8. The method of claim 6, wherein the plurality of interactive technologies includes Short message Services (SMS).

9. The method of claim 6, wherein the plurality of interactive technologies includes SIM Toolkit (STK).

10. The method of claim 6, wherein the plurality of interactive technologies includes Unstructured Supplementary Services Data (USSD).

11. The method of claim 6, wherein the plurality of interactive technologies includes Wireless Application Protocol (WAP).

12. The method of claim 1, further comprising, using a plurality of wired and/or wireless network transport mechanisms to route a purchase request, wherein GSM is just one of the plurality of network transport mechanisms.

13. The method of claim 12, wherein the plurality of network transport mechanisms includes CDMA.

14. The method of claim 12, wherein the plurality of network transport mechanisms includes TDMA.

15. The method of claim 12, wherein the plurality of network transport mechanisms includes GPRS.

16. The method of claim 12, wherein the plurality of network transport mechanisms includes 3G.

17. The method of claim 12, wherein the plurality of network transport mechanisms includes Bluetooth.

18. The method of claim 12, wherein the plurality of network transport mechanisms includes Infrared.

19. The method of claim 12, wherein the plurality of network transport mechanisms includes RFID.

20. The method of claim 12, wherein the plurality of network transport mechanisms includes Internet.

21. The method of claim 1, further comprising, inserting a plurality of cardholder credentials into an HTML authentication request page and/or message; wherein a PIN is just one of the plurality of credentials.

22. The method of claim 21, wherein the plurality of credentials includes a user Id and/or password.

23. The method of claim 21, wherein the plurality of credentials includes a biometric.

24. The method of claim 21, wherein the plurality of credentials includes a pseudo random number.

25. The method of claim 21, wherein the plurality of credentials includes a cryptogram.

26. The method of claim 21, wherein the plurality of credentials includes a digital signature.

27. The method of claims 21 to 26, further comprising receiving information related to a plurality of credentials, verifying the plurality of credentials based on the received information, and authenticating the transaction based on a successful verification of the plurality of credentials.

28. A method of authenticating a transaction initiated from a non-internet enabled device substantially as herein described and illustrated with reference to the attached drawings

29. A system for authenticating a transaction initiated from a non-internet enabled device substantially as herein described and illustrated with reference to the attached drawings

30. A method of enabling Issuers, Acquirers and Merchants to use the 3-D Secure™ online cardholder authentication protocol to authenticate cardholders transacting with non-internet enabled devices. The invention operates as a proxy on behalf of the cardholder and simulates a core 3-D Secure™ session to the Merchant Plug-in (MPI) and Issuer Access Control Server (ACS). That is, it converts voice or data based messages received from a non-internet enabled device into a set of messages that are consistent with the requirements of the 3-D Secure™ protocol. Further, the invention can be implemented without Issuers, Acquirers or Merchants having to upgrade or enhance infrastructure.

31. A system for enabling Issuers, Acquirers and Merchants to use the 3-D Secure™ online cardholder authentication protocol to authenticate cardholders transacting with non-internet enabled devices. The invention operates as a proxy on behalf of the cardholder and simulates a core 3-D Secure™ session to the Merchant Plug-in (MPI) and Issuer Access Control Server (ACS). That is, it converts voice or data based messages received from a non-internet enabled device into a set of messages that are consistent with the requirements of the 3-D Secure™ protocol. Further, the invention can be implemented without Issuers, Acquirers or Merchants having to upgrade or enhance infrastructure.

Patent

ABSTRACT

[031] A method of enabling Issuers, Acquirers and Merchants to use the 3-D Secure™ online cardholder authentication protocol to authenticate cardholders transacting with non-internet enabled devices. The invention operates as a proxy on behalf of the cardholder and simulates a core 3-D Secure™ session to the Merchant Plug-in (MPI) and Issuer Access Control Server (ACS). That is, it converts voice or data based messages received from a non-internet enabled device into a set of messages that are consistent with the requirements of the 3-D Secure™ protocol. Further, the invention can be implemented without Issuers, Acquirers or Merchants having to upgrade or enhance infrastructure.

Figure 1

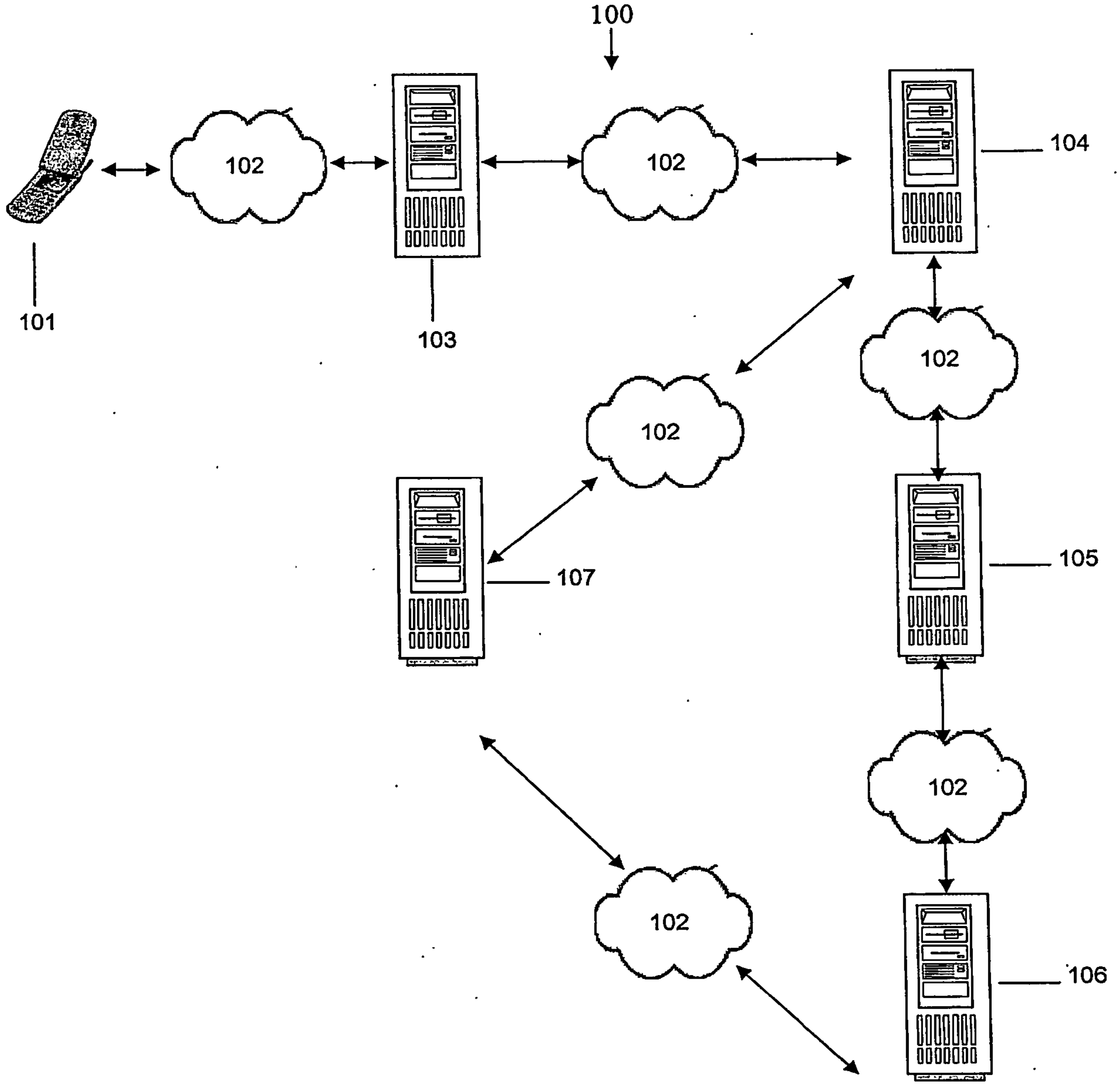
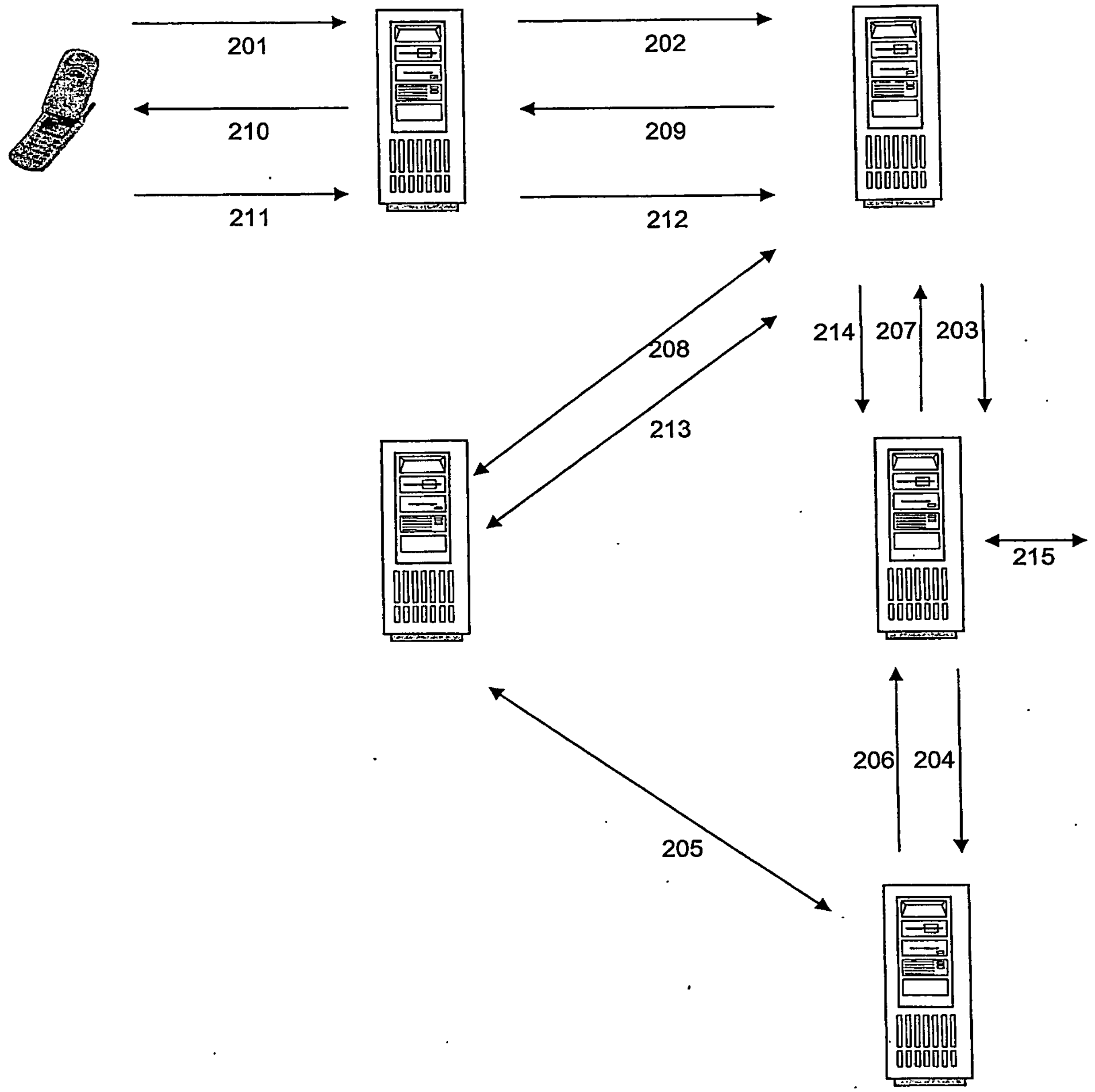


Figure 2


201
202
210
209
211
212
208
214
207
203
213
215
206
204
205